# The Frobenius formalism in Galois quantum systems

A. Vourdas
*Department of Computing, University of Bradford, Bradford BD7 1DP, United Kingdom*

**Abstract.** Quantum systems in which the position and momentum take values in the ring $\mathcal{Z}_d$ and which are described with $d$-dimensional Hilbert space, are considered. When $d$ is the power of a prime, the position and momentum take values in the Galois field $GF(p^\ell)$, the position-momentum phase space is a finite geometry and the corresponding 'Galois quantum systems' have stronger properties. The study of these systems uses ideas from the subject of field extension in the context of quantum mechanics. The Frobenius automorphism in Galois fields leads to Frobenius subspaces and Frobenius transformations in Galois quantum systems. Links between the Frobenius formalism and Riemann surfaces, are discussed.

**Keywords:** Galois fields, Quantum Mechanics, Applied Harmonic Analysis

**JEL codes:** 81S30; 11S20

## 1. Introduction

Phase space methods play an important role in quantum mechanics. In the case of a harmonic oscillator, both the position $x$ and the momentum $p$ take values in $R$ (real numbers) and the position-momentum phase space is the plane $R \times R$. The state $|f\rangle$ of the system is described with the wavefunction $f(x)$ in the x-representation, or with the wavefunction $\tilde{f}(p)$ in the p-representation. These two wavefunctions are related through the Fourier transform:

$$\tilde{f}(p) = (2\pi)^{-1/2} \int dx f(x) \exp(-ixp)$$
$$\int dx |f(x)|^2 = \int dp |\tilde{f}(p)|^2 = 1 \qquad (1)$$

The states $|f\rangle$ belong in an infinite-dimensional Hilbert space. There are two important classes of transformations in the phase space $R \times R$. The first is displacements and they are associated with the Heisenberg-Weyl group; and the second is symplectic transformations and they are associated with the symplectic group $Sp(2, R)$.

In this article we are interested in quantum systems described with finite-dimensional Hilbert spaces. These systems have been studied originally by Weyl[1] and Schwinger[2], and later by many authors [3, 4, 5, 6, 7, 8, 9, 10]. A review of the subject with an extensive

list of references has been given in [11]. In this case the position and momentum take values in the ring $\mathcal{Z}_d$ (the integers modulo $d$) and the phase space of the system is the toroidal lattice $\mathcal{Z}_d \times \mathcal{Z}_d$. Displacements in this phase space are discrete and form a Heisenberg-Weyl group.

The next step is to try to define symplectic transformations. We note however that the $\mathcal{Z}_d \times \mathcal{Z}_d$ phase space is in general a collection of points with no geometrical structure and we cannot define symplectic transformations. Consequently the properties of such systems are weaker in comparison to the harmonic oscillator. The root of these difficulties is that $\mathcal{Z}_d$ is a ring. However when the dimension $d$ of the Hilbert space of the system is the power of a prime number $p$ (i.e., $d = p^\ell$) the $\mathcal{Z}_d$ (with appropriate multiplication rule) becomes the Galois field $GF(p^\ell)$. In this case the phase space is a finite geometry [12] and translations and rotations are well defined and they form groups. In this case we can define the group of symplectic transformations $Sp(2, GF(p^\ell))$[8].

Another problem which leads to similar ideas through another route, is to find mutually unbiased bases (orthonormal bases $|a_i\rangle$ and $|b_j\rangle$ such that $|\langle a_i|b_j\rangle|^2 = d^{-1}$)[13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23]. It is known that the number of such bases cannot exceed $d+1$; and it is also known that for systems where $d$ is the power of a prime, the number of such bases is indeed $d+1$. Related to this is also the so-called 'mean king's problem'[24, 25].

Galois fields play a central role in classical coding and these techniques could be transfered in quantum information processing. Work with Galois fields in the context of quantum coding has been reported in [26, 27, 28].

In summary, Galois fields in finite quantum systems have been introduced either in order to have well defined symplectic transformations; or in the context of mutually unbiased bases; or in the context of quantum coding. In this paper we are interested in the use of Galois fields in quantum mechanics, as a subject in its own right rather than as an application driven problem. Most of the material presented here has appeared in the literature from a different point of view. The aim of this review article is to present these ideas with a different emphasis and promote the interaction between Galois fields and quantum mechanics.

We transfer the concept of field extension in the context of Hilbert spaces. We start with a $p$-dimensional Hilbert space $\mathcal{H}$ (where $p$ is an odd prime number) and through tensor product of $\ell$ such spaces, we construct a $p^\ell$-dimensional Hilbert space $H$. In this space the Fourier transform $F$ is defined in terms of additive characters in $GF(p^\ell)$ and is different from $\mathcal{F} \otimes ... \otimes \mathcal{F}$, where $\mathcal{F}$ is the Fourier transform in $\mathcal{H}$. The Fourier transform $F$ is very important because it provides the 'Galois identity' to these systems. We then develop concepts like Galois conju-

gate position (and momentum) states; Frobenius subspaces; Frobenius transformations, etc. Frobenius automorphisms play an important role in Galois fields; and here we develop analogous concepts in Hilbert spaces in the context of quantum mechanics (and in the related area of applied harmonic analysis). We also explain that there are interesting connections between the Frobenius formalism in Galois theory and Riemann surfaces.

In section 2 we present some ideas from the theory of Galois fields, in the language of matrices. In section 3 we discuss the basic theory of general systems with finite Hilbert space. Galois quantum systems are discussed in section 4. An important part of Galois theory is the Frobenius transformations and their implications in the present context are studied in section 5. Links between the Frobenius formalism in a quantum mechanical context and Riemann surfaces are discussed in section 6. We conclude in section 7 with a discussion of our results.

.

## 2. Galois fields

We consider the Galois field $GF(p^\ell)$. Its elements can be written as polynomials:

$$\alpha = \alpha_0 + \alpha_1\epsilon + ... + \alpha_{\ell-1}\epsilon^{\ell-1}; \qquad \alpha_0, \alpha_1, ..., \alpha_{\ell-1} \in \mathcal{Z}_p \tag{2}$$

These polynomials are defined modulo an irreducible polynomial of degree $\ell$:

$$P(\epsilon) \equiv c_0 + c_1\epsilon + ... + c_{\ell-1}\epsilon^{\ell-1} + \epsilon^\ell; \qquad c_0, c_1, ..., c_{\ell-1} \in \mathcal{Z}_p \tag{3}$$

Different irreducible polynomials of the same degree $\ell$ lead to isomorphic finite fields. Results of practical calculations do depend on the choice of the irreducible polynomial, but different choices lead to isomorphic results.

The powers $\alpha$, $\alpha^p$,...,$\alpha^{p^{\ell-1}}$ are Galois conjugates. The elements of the base field $\mathcal{Z}_p$ are Galois self-conjugates. The trace of $\alpha$ is the sum of all its conjugates:

$$\mathrm{Tr}(\alpha) = \alpha + \alpha^p + ... + \alpha^{p^{\ell-1}}; \qquad \mathrm{Tr}(\alpha) \in \mathcal{Z}_p \tag{4}$$

All conjugates have the same trace.

We consider a nonzero constant $\mathfrak{h}$ in $GF(p^\ell)$ which we call 'inverse Planck's constant' because later will play such a role in quantum systems. For practical calculations we introduce the:

$$\mathcal{E}_\lambda \equiv \mathrm{Tr}(\mathfrak{h}\epsilon^\lambda); \qquad \mathcal{E}_\lambda \in \mathcal{Z}_p \tag{5}$$

We also introduce the following $\ell \times \ell$ matrices with elements in $\mathcal{Z}_p$:

$$g_{\lambda\kappa} \equiv \mathcal{E}_{\lambda+\kappa}; \qquad G_{\kappa\lambda} \equiv (g^{-1})_{\kappa\lambda}; \qquad G_{\kappa\lambda} \in \mathcal{Z}_p \tag{6}$$

We note that the determinant of $g$ is non-zero and therefore its inverse $G$ exists.

The $GF(p^\ell)$ can be regarded as a $\ell$-dimensional vector space with the $1, \epsilon, \epsilon^2, ..., \epsilon^{\ell-1}$ as a basis. We can change this basis into a different basis, and for later use we introduce the dual basis $E_0, E_1, ..., E_{\ell-1}$, as follows:

$$E_\kappa = \sum_\lambda G_{\kappa\lambda}\epsilon^\lambda; \qquad \mathrm{Tr}(\mathfrak{h}\epsilon^\kappa E_\lambda) = \delta_{\kappa\lambda} \tag{7}$$

A number $\alpha \in GF(p^\ell)$ can be expressed in the two bases as:

$$\begin{aligned} \alpha &= \sum_{\lambda=0}^{\ell-1} \alpha_\lambda \epsilon^\lambda = \sum_{\lambda=0}^{\ell-1} \bar{\alpha}_\lambda E_\lambda \\ \alpha_\lambda &= \mathrm{Tr}[\mathfrak{h}\alpha E_\lambda]; \qquad \bar{\alpha}_\lambda = \mathrm{Tr}[\mathfrak{h}\alpha\epsilon^\lambda] \end{aligned} \tag{8}$$

We refer to $\alpha_\lambda$ and $\bar{\alpha}_\lambda$ as the components and dual components of $\alpha$, correspondingly. They are related as follows:

$$\alpha_\lambda = \sum_\kappa G_{\lambda\kappa}\bar{\alpha}_\kappa; \qquad \bar{\alpha}_\lambda = \sum_\kappa g_{\lambda\kappa}\alpha_\kappa \tag{9}$$

The trace of $\mathfrak{h}\alpha$ is given by

$$\mathrm{Tr}(\mathfrak{h}\alpha) = \sum_{\lambda=0}^{\ell-1} \alpha_\lambda \mathcal{E}_\lambda \tag{10}$$

If $\beta$ is another number in $GF(p^\ell)$

$$\beta = \sum_{\lambda=0}^{\ell-1} \beta_\lambda \epsilon^\lambda = \sum_{\lambda=0}^{\ell-1} \bar{\beta}_\lambda E_\lambda \tag{11}$$

the trace of $\mathfrak{h}\alpha\beta$ is given by

$$\begin{aligned} \mathrm{Tr}(\mathfrak{h}\alpha\beta) &= \sum_{\lambda,\kappa} g_{\lambda\kappa}\alpha_\lambda\beta_\kappa = \sum_{\lambda,\kappa} G_{\lambda\kappa}\bar{\alpha}_\lambda\bar{\beta}_\kappa \\ &= \sum_\lambda \alpha_\lambda\bar{\beta}_\lambda = \sum_\lambda \bar{\alpha}_\lambda\beta_\lambda \end{aligned} \tag{12}$$

## 2.1. Galois conjugates

For practical calculations of the Galois conjugates we introduce the $\ell \times \ell$ matrix $\mathcal{C}$ with elements in $\mathcal{Z}_p$, through the relations:

$$\epsilon^{\mu p} = \sum_{\kappa=0}^{\ell-1} \epsilon^{\kappa} \mathcal{C}_{\kappa\mu} \tag{13}$$

Here $\kappa, \mu$ take values from 0 to $\ell - 1$. We can show that more generally

$$\epsilon^{\mu p^{\lambda}} = \sum_{\kappa=0}^{\ell-1} \epsilon^{\kappa} (\mathcal{C}^{\lambda})_{\kappa\mu} \tag{14}$$

where $\lambda$ take values from 0 to $\ell - 1$. For $\lambda = 0$ we have $\mathcal{C}^0 = \mathbf{1}$. Also

$$\mathcal{C}^{\ell} = \mathbf{1}; \qquad \mathcal{C}_{\kappa 0} = \delta(\kappa, 0) \tag{15}$$

where $\delta$ is the Kronecker delta. We can now express the conjugates of the arbitrary number $\alpha$ of Eq.(2) as

$$\alpha^{p^{\lambda}} = \sum_{\kappa,\mu} \epsilon^{\kappa} (\mathcal{C}^{\lambda})_{\kappa\mu} \alpha_{\mu} \tag{16}$$

The Frobenius map

$$\sigma : \alpha \ \rightarrow \ \alpha^{p} \tag{17}$$

defines an automorphism in $GF(p^{\ell})$. It maps the Galois conjugates to each other and leaves all elements of the base field $\mathcal{Z}_p$ fixed. The Frobenius map can be written in terms of the components of $\alpha$ and $\alpha^p$ as:

$$\sigma : \alpha_{\kappa} \ \rightarrow \ \sum_{\mu} \mathcal{C}_{\kappa\mu} \alpha_{\mu} \tag{18}$$

## 2.2. Characters

Below we will use the complex-valued function

$$\chi(\alpha) = \omega[\mathrm{Tr}(\alpha)]; \qquad \omega = \exp\left(i \frac{2\pi}{p}\right) \tag{19}$$

This is an additive character in $GF(p^{\ell})$:

$$\chi(\alpha)\chi(\beta) = \chi(\alpha + \beta); \qquad \alpha, \beta \in GF(p^{\ell}) \tag{20}$$

We can easily show that for $n, m, r \in GF(p^\ell)$:

$$\frac{1}{p^\ell}\sum_n \omega\left[\mathrm{Tr}(nm-nr)\right]=\delta(m,r) \tag{21}$$

A more general relation is

$$\frac{1}{p^\ell}\sum_n \omega\left[\mathrm{Tr}(nm-n^{p^\lambda}r)\right]=\delta\left(m,r^{p^{\ell-\lambda}}\right)=\delta\left(m^{p^\lambda},r\right) \tag{22}$$

We note that in terms of the components of the $m^{p^\lambda}, r$

$$\delta\left(m^{p^\lambda},r\right)=\prod_{\kappa=0}^{\ell-1}\delta\left(\sum_\mu (\mathcal{C}^\lambda)_{\kappa\mu}m_\mu, r_\kappa\right) \tag{23}$$

### 2.3. Example

We consider the Galois fields $GF(9)$ and calculate the quantities defined above for the irreducible polynomial $\epsilon^2+\epsilon+2$. We find that

$$\mathcal{C}=\begin{pmatrix}1 & -1\\ 0 & -1\end{pmatrix} \tag{24}$$

We also choose $\mathfrak{h}=1$ and find that

$$\mathcal{E}_0=-1; \quad \mathcal{E}_1=-1; \quad \mathcal{E}_2=0 \tag{25}$$

In this case

$$g=\begin{pmatrix}-1 & -1\\ -1 & 0\end{pmatrix}; \quad G=\begin{pmatrix}0 & -1\\ -1 & 1\end{pmatrix} \tag{26}$$

If we choose $\mathfrak{h}=1+\epsilon$ we find that

$$\mathcal{E}_0=1; \quad \mathcal{E}_1=-1; \quad \mathcal{E}_2=-1 \tag{27}$$

In this case

$$g=\begin{pmatrix}1 & -1\\ -1 & -1\end{pmatrix}; \quad G=\begin{pmatrix}-1 & 1\\ 1 & 1\end{pmatrix} \tag{28}$$

## 3. Finite quantum systems

We consider a quantum system with a $d$-dimensional Hilbert space $\mathcal{H}$. A physical example is a system with spin $j$ for which $d=2j+1$. We

consider an orthonormal basis of 'position states' which we denote as $|\mathcal{X};m\rangle$ where $m$ takes values in the ring $\mathcal{Z}_d$. Here $\mathcal{X}$ is not a variable, but it simply indicates position states. Through a Fourier transform we will define the 'momentum basis' $|\mathcal{P};m\rangle$ and the position-momentum phase space.

### 3.1. Fourier transforms

The Fourier transform is defined as:

$$\mathcal{F} = d^{-1/2} \sum_{m=0}^{d-1} \sum_{n=0}^{d-1} \omega(mn) |\mathcal{X};m\rangle\langle\mathcal{X};n| \tag{29}$$

where

$$\omega(\alpha) \equiv \omega^{\alpha} = \exp\left[i\frac{2\pi\alpha}{d}\right] \tag{30}$$

The Fourier transform obeys the relation:

$$\mathcal{F}^4 = \mathbf{1} \tag{31}$$

The momentum states are defined as

$$|\mathcal{P};m\rangle = \mathcal{F}|\mathcal{X};m\rangle = d^{-1/2} \sum_{n} \omega(mn)|\mathcal{X};n\rangle \tag{32}$$

and they form another orthonormal basis in $\mathcal{H}$. The position-momentum phase space is the toroidal lattice $\mathcal{Z}_d \times \mathcal{Z}_d$.

Position and momentum operators $\hat{x}$ and $\hat{p}$ are defined as

$$\hat{x} = \sum_{n=0}^{d-1} n|\mathcal{X};n\rangle\langle\mathcal{X};n|; \qquad \hat{p} = \sum_{n=0}^{d-1} n|\mathcal{P};n\rangle\langle\mathcal{P};n|; \qquad \hat{p} = \mathcal{F}\hat{x}\mathcal{F}^{\dagger} \tag{33}$$

### 3.2. Displacements

In the $\mathcal{Z}_d \times \mathcal{Z}_d$ phase space we define the displacement operators

$$\begin{aligned} \mathcal{Z} &= \omega^{\hat{x}} = \sum_{n=0}^{d-1} \omega(n)|\mathcal{X};n\rangle\langle\mathcal{X};n| \\ \mathcal{X} &= \omega^{-\hat{p}} = \sum_{n=0}^{d-1} \omega(-n)|\mathcal{P};n\rangle\langle\mathcal{P};n| \end{aligned} \tag{34}$$

They are displacement operators in the sense that:

$$\mathcal{Z}^{\alpha}|\mathcal{P};m\rangle = |\mathcal{P};m+\alpha\rangle; \qquad \mathcal{Z}^{\alpha}|\mathcal{X};m\rangle = \omega(\alpha m)|\mathcal{X};m\rangle \tag{35}$$

$$\mathcal{X}^\beta|\mathcal{P};m\rangle=\omega(-m\beta)|\mathcal{P};m\rangle;\qquad \mathcal{X}^\beta|\mathcal{X};m\rangle=|\mathcal{X};m+\beta\rangle \tag{36}$$

Powers of the displacements operators form the Heisenberg-Weyl group. Indeed we can show that the displacement operators obey the relations

$$\mathcal{X}^d=\mathcal{Z}^d=\mathbf{1};\qquad \mathcal{X}^\beta\mathcal{Z}^\alpha=\mathcal{Z}^\alpha\mathcal{X}^\beta\omega(-\alpha\beta) \tag{37}$$

where $\alpha$,$\beta$ are integers in $\mathcal{Z}_d$. General displacement operators are defined as

$$\mathcal{D}(\alpha,\beta)=\mathcal{Z}^\alpha\mathcal{X}^\beta\omega(-2^{-1}\alpha\beta) \tag{38}$$

## 4. Quantum systems with dimension $d=p^\ell$

### 4.1. Galois quantum systems

We have considered quantum systems with position in the ring $\mathcal{Z}_d$. When $d=p$ (where $p$ is a prime number) the $\mathcal{Z}_p$ is a field. We will use the concept of field extension to introduce quantum systems with position in the Galois field $GF(p^\ell)$. In doing so we combine ideas from Galois fields, Fourier transform, quantum mechanics and applied harmonic analysis.

Let $\mathcal{H}$ be $p$-dimensional Hilbert space, where $p$ is an odd prime. We consider the tensor product

$$H=\mathcal{H}\otimes...\otimes\mathcal{H} \tag{39}$$

of $\ell$ such spaces and use calligraphic letters for operators and states on the various $p$-dimensional Hilbert spaces $\mathcal{H}$; and ordinary letters for operators and states on the $p^\ell$-dimensional Hilbert space $H$.

The position states in $H$ can be labeled with $m\in GF(p^\ell)$ in the following way:

$$|X;m\rangle\ \equiv\ |\mathcal{X};m_0\rangle\otimes...\otimes|\mathcal{X};m_{\ell-1}\rangle \tag{40}$$

where the notation of Eq.(8) is used for the components of $m$. This is, of course, a trivial labeling rule. Galois theory ideas enter into quantum systems when we introduce the Fourier transform as:

$$\begin{aligned} F\ &=\ (p^\ell)^{-1/2}\sum_{m,n}\omega[\mathrm{Tr}(\mathfrak{h}mn)]|X;m\rangle\langle X;n| \\ \omega\ &=\ \exp\left(i\frac{2\pi}{p}\right);\qquad F^4=\mathbf{1} \end{aligned} \tag{41}$$

The characters of Eq.(19) enter in this Fourier transform. $\mathfrak{h}$ plays the role of the inverse Planck's constant.

Acting with this Fourier transform on position states we get momentum states

$$\begin{aligned} |P;m\rangle &= F|X;m\rangle = (p^\ell)^{-1/2}\sum_n \omega[\mathrm{Tr}(\mathfrak{h}mn)]|X;n\rangle \\ &= |\mathcal{P};\bar{m}_0\rangle\otimes ...\otimes|\mathcal{P};\bar{m}_{\ell-1}\rangle \end{aligned} \tag{42}$$

The dual components $\bar{m}_i$ of $m$ enter in the momentum states, while the components $m_i$ enter in the position states.

We note that $|P;m\rangle$ is different from $|\mathcal{P};m_0\rangle\otimes ...\otimes|\mathcal{P};m_{\ell-1}\rangle$. Related to this is the fact that $F$ is different from the operator $\mathcal{F}\otimes ...\otimes\mathcal{F}$. Indeed

$$F=\sum_m |\mathcal{P};\bar{m}_0\rangle\langle\mathcal{X};m_0|\otimes ...\otimes|\mathcal{P};\bar{m}_{\ell-1}\rangle\langle\mathcal{X};m_{\ell-1}| \tag{43}$$

and

$$\mathcal{F}\otimes ...\otimes\mathcal{F}=\sum_m |\mathcal{P};m_0\rangle\langle\mathcal{X};m_0|\otimes ...\otimes|\mathcal{P};m_{\ell-1}\rangle\langle\mathcal{X};m_{\ell-1}| \tag{44}$$

We stress that a Galois quantum system with Hilbert space $H$, Fourier transform $F$ and positions (and momenta) in $GF(p^\ell)$ is different from a quantum system with the same Hilbert space $H$ but with Fourier transform $\mathcal{F}\otimes ...\otimes\mathcal{F}$ and positions (and momenta) in $\mathcal{Z}_p\times ...\times\mathcal{Z}_p$.

The position operator is defined as:

$$\hat{x}=\sum_m m|X;m\rangle\langle X;m|=\sum_\lambda \epsilon^\lambda\left[\mathbf{1}\otimes ...\otimes x_{(\lambda)}\otimes ...\otimes\mathbf{1}\right] \tag{45}$$

With a Fourier transform we can define the momentum operator as:

$$\begin{aligned} \hat{p} &= F\hat{x}F^\dagger=\sum_m m|P;m\rangle\langle P;m| \\ &= \sum_\lambda E_\lambda\left[\mathbf{1}\otimes ...\otimes p_{(\lambda)}\otimes ...\otimes\mathbf{1}\right] \end{aligned} \tag{46}$$

Their eigenvalues obey the relation $m^{p^\ell}=m$ and therefore according to the Cayley-Hamilton theorem:

$$\hat{x}^{p^\ell}=\hat{x};\qquad \hat{p}^{p^\ell}=\hat{p} \tag{47}$$

### 4.2. Example

As an example we consider the $GF(9)$ and we choose the irreducible polynomial $\epsilon^2+\epsilon+2$, as in section 2.3. We consider the position state

$$|X;1+\epsilon\rangle=|\mathcal{X};1\rangle\otimes|\mathcal{X};1\rangle \tag{48}$$

For $\mathfrak{h}=1$, the dual basis is $E_0=-\epsilon$ and $E_1=-1+\epsilon$. Therefore $1+\epsilon=E_0-E_1$ and

$$|P;1+\epsilon\rangle=F|X;1+\epsilon\rangle=|\mathcal{P};1\rangle\otimes|\mathcal{P};-1\rangle \tag{49}$$

For $\mathfrak{h}=1+\epsilon$, the dual basis is $E_0=1-\epsilon$ and $E_1=1+\epsilon$. Therefore

$$|P;1+\epsilon\rangle=F|X;1+\epsilon\rangle=|\mathcal{P};0\rangle\otimes|\mathcal{P};1\rangle \tag{50}$$

### 4.3. Displacements in Galois quantum systems

We define the displacement operators

$$\begin{aligned} Z &= \sum_n \omega[\mathrm{Tr}(\mathfrak{h}n)]|X;n\rangle\langle X;n| \\ X &= \sum_n \omega[-\mathrm{Tr}(\mathfrak{h}n)]|P;n\rangle\langle P;n| \end{aligned} \tag{51}$$

We are interested in more general powers $Z^\alpha$ and $X^\beta$ where $\alpha,\beta\in GF(p^\ell)$. We can easily prove that for $\alpha,\beta\in\mathcal{Z}_p$ the powers $Z^\alpha$ and $X^\beta$ are given by:

$$\begin{aligned} Z^\alpha &= \sum_n \omega[\mathrm{Tr}(\mathfrak{h}\alpha n)]|X;n\rangle\langle X;n| \\ X^\beta &= \sum_n \omega[-\mathrm{Tr}(\mathfrak{h}\beta n)]|P;n\rangle\langle P;n| \end{aligned} \tag{52}$$

But for $\alpha,\beta\in GF(p^\ell)$ we need to define the meaning of a complex matrix to a power which belongs in a Galois field. In this case Eq.(52) is a definition for $Z^\alpha$ and $X^\beta$.

We next show that

$$Z^\alpha|P;m\rangle=|P;m+\alpha\rangle;\qquad Z^\alpha|X;m\rangle=\omega[\mathrm{Tr}(\mathfrak{h}\alpha m)]|X;m\rangle \tag{53}$$

$$X^\beta|P;m\rangle=\omega[-\mathrm{Tr}(\mathfrak{h}m\beta)]|P;m\rangle;\qquad X^\beta|X;m\rangle=|X;m+\beta\rangle \tag{54}$$

They are analogous to Eqs(35),(36) with an extra trace. We also show

$$X^\beta Z^\alpha=Z^\alpha X^\beta\omega[-\mathrm{Tr}(\mathfrak{h}\alpha\beta)] \tag{55}$$

This is analogous to Eq.(37) with an extra trace.

General displacement in the $GF(p^\ell)\times GF(p^\ell)$ phase space, are defined as:

$$D(\alpha,\beta)=Z^\alpha X^\beta\omega\left[-\frac{1}{2}\mathrm{Tr}(\mathfrak{h}\alpha\beta)\right] \tag{56}$$

There is an interesting relation between the displacement operators acting on $H$ and the displacement operators $\mathcal{D}$ of Eq. (38) acting on the various $p$-dimensional Hilbert spaces $\mathcal{H}$:

$$D(\alpha,\beta) \;=\; \mathcal{D}(\bar{\alpha}_0,\beta_0)\otimes ...\otimes \mathcal{D}(\bar{\alpha}_{\ell-1},\beta_{\ell-1}) \tag{57}$$

Here $\bar{\alpha}_i$ are the dual components of $\alpha$ and $\beta_i$ are the components of $\beta$ as in Eq.(8).

## 5. Frobenius formalism

### 5.1. Frobenius automorphism and irreducible polynomials

The product

$$f(y)\equiv (y-\alpha)(y-\alpha^p)...(y-\alpha^{p^{\ell-1}}) \tag{58}$$

involves all the Galois conjugates and is an irreducible polynomial of degree $\ell$ in $\mathcal{Z}_p[y]$ (the polynomials with coefficients in $\mathcal{Z}_p$).

The product of all distinct irreducible polynomials in $\mathcal{Z}_p[y]$ of degree $d$, where $d$ is a divisor of $\ell$, is:

$$\prod f_i(y) = y^{p^\ell}-y \tag{59}$$

For simplicity, $\ell$ is taken below to be a prime number. In this case the $\mathcal{Z}_p$ is the only proper subfield of $GF(p^\ell)$ and we have a two-layer structure with a total of $p+s$ irreducible polynomials, where

$$s=\frac{p^\ell-p}{\ell}. \tag{60}$$

The first layer has $s$ irreducible polynomials with degree $\ell$; and to each of them correspond $\ell$ Galois conjugates. We label them with $i=0,...,s-1$. The second layer has the $p$ polynomials $f_i(y)=y-m$ where $m\in\mathcal{Z}_p$. We label them with $i=s,...,s+p-1$. Their product is

$$\prod_{i=0}^{s-1} f_i(y)=\frac{y^{p^\ell}-y}{y^p-y};\qquad \prod_{i=s}^{s+p-1} f_i(y)=y^p-y. \tag{61}$$

The fact that $\mathcal{Z}_p$ is a subfield of $GF(p^\ell)$ implies that the $y^p-y$ divides the $y^{p^\ell}-y$.

### 5.2. Frobenius subspaces

The Frobenius automorphism is central in Galois formalism and in this section we study its implications in our context. We show that the full Hilbert space splits naturally into 'Frobenius subspaces' comprised by states labelled with Galois conjugates. We also construct transformations which leave these subspaces invariant.

We call conjugate position states the ones which are labelled with Galois conjugate numbers. They are the states

$$|X;m^{p^\lambda}\rangle \equiv |\mathcal{X};\sum_\mu (\mathcal{C}^\lambda)_{0,\mu} m_\mu\rangle \otimes ... \otimes |\mathcal{X};\sum_\mu (\mathcal{C}^\lambda)_{\ell-1,\mu} m_\mu\rangle \quad (62)$$

where $\lambda$ takes the values $0,...,\ell-1$. We split the Hilbert space $H$ into subspaces, each of which is spanned by conjugate position states. All conjugates correspond to a particular irreducible polynomial and we label each of these subspaces with the index of the corresponding irreducible polynomial. For the irreducible polynomial

$$f_i(y) = (y-m)(y-m^p)...(y-m^{p^{\ell-1}}) \quad (63)$$

we consider the space

$$H_{Xi} = \text{span}\{|X;m\rangle, |X;m^p\rangle, ..., |X;m^{p^{\ell-1}}\rangle\} \quad (64)$$

The index $i$ indicates the corresponding irreducible polynomial and the index $X$ indicates that the position states have been used. We can use the states $U|X;m\rangle$ where $U$ is any unitary operator, and we will get different Frobenius subspaces which we denote as $H_{UXi}$. We call $\Pi_{Xi}$ the projection operator to the space $H_{Xi}$.

The Hilbert space $H$ is the direct sum of all Frobenius subspaces. For prime $\ell$, there are $s$ Frobenius subspaces which are $\ell$-dimensional and we call $H_A$ their direct sum; and there are $p$ Frobenius subspaces which are one-dimensional and we call $H_B$ their direct sum:

$$H = H_A \bigoplus H_B; \qquad H_A = \bigoplus_{i=0}^{s-1} H_{Xi}; \qquad H_B = \bigoplus_{i=s}^{s+p-1} H_{Xi} \quad (65)$$

### 5.3. Frobenius transformations

We call Frobenius transformations the following unitary transformations in $H_{Xi}$:

$$\mathcal{G}_i \equiv \sum_{\lambda\in\mathcal{Z}_\ell} |X;m^{p^{\lambda+1}}\rangle\langle X;m^{p^\lambda}| \quad (66)$$

Here $m$ is one of the Galois conjugates corresponding to the irreducible polynomial $f_i(y)$ and by taking all $\lambda \in \mathcal{Z}_\ell$ we get all the Galois conjugates. For the one dimensional spaces $H_{Xi}$, the $\mathcal{G}_i$ is simply the projection operator $\Pi_{Xi}$:

$$\mathcal{G}_i = \Pi_{Xi}; \qquad i = s, ..., s+p-1 \tag{67}$$

We sum all the transforms $\mathcal{G}_i$ and we get

$$\mathcal{G} = \sum_{i=0}^{s+p-1} \mathcal{G}_i \tag{68}$$

We can show that

$$\mathcal{G}^\ell = \mathbf{1}; \qquad [\mathcal{G}, \Pi_{Xi}] = 0 \tag{69}$$

The operators $\mathcal{G}^\lambda$ map the position state $|X; m\rangle$ to its Galois conjugate position states $|X; m^{p^\lambda}\rangle$. We can express this in terms of the various components of these states as:

$$\begin{aligned} &\mathcal{G}^\lambda |\mathcal{X}; m_0\rangle \otimes ... \otimes |\mathcal{X}; m_{\ell-1}\rangle \\ &= |\mathcal{X}; \sum_\mu (\mathcal{C}^\lambda)_{0,\mu} m_\mu\rangle \otimes ... \otimes |\mathcal{X}; \sum_\mu (\mathcal{C}^\lambda)_{\ell-1,\mu} m_\mu\rangle \end{aligned} \tag{70}$$

We can show that

$$\mathcal{G}^\lambda X^\beta (\mathcal{G}^\dagger)^\lambda = X^{\beta^{p^\lambda}}; \qquad \mathcal{G}^\lambda Z^\alpha (\mathcal{G}^\dagger)^\lambda = Z^{\alpha^{p^\lambda} \mathfrak{h}^{p^\lambda - 1}} \tag{71}$$

and more generally that

$$\mathcal{G}^\lambda D(\alpha, \beta)(\mathcal{G}^\dagger)^\lambda \;=\; D\left(\alpha^{p^\lambda} \mathfrak{h}^{p^\lambda - 1}, \beta^{p^\lambda}\right) \tag{72}$$

where $\lambda \in \mathcal{Z}_\ell$. When $\alpha, \beta \in \mathcal{Z}_p$ the $\mathcal{G}$ commutes with $D(\alpha, \beta)$. We note here that although $\mathcal{G}$ commutes with $X$ and $Z$, it does **not** commute with its powers $X^\alpha$ and $Z^\alpha$ when $\alpha \in GF(p^\ell)$.

We next use Eq.(16) and the relation

$$\alpha^{p^\lambda} \mathfrak{h}^{p^\lambda - 1} = \sum_\mu A_\mu E_\mu; \qquad A_\mu \equiv \sum_\kappa \bar{\alpha}_\kappa (\mathcal{C}^{-\lambda})_{\kappa\mu} \tag{73}$$

and taking into account Eq.(57) we rewrite Eq.(72) as:

$$\begin{aligned} &\mathcal{G}^\lambda \mathcal{D}(\bar{\alpha}_0, \beta_0) \otimes ... \otimes \mathcal{D}(\bar{\alpha}_{\ell-1}, \beta_{\ell-1})(\mathcal{G}^\dagger)^\lambda = \\ &\mathcal{D}\left(A_0, \sum_\mu (\mathcal{C}^\lambda)_{0,\mu} \beta_\mu\right) \otimes ... \otimes \mathcal{D}\left(A_{\ell-1}, \sum_\mu (\mathcal{C}^\lambda)_{\ell-1,\mu} \beta_\mu\right) \end{aligned} \tag{74}$$

## 5.4. Quantum formalism in $\mathfrak{H}_{X\kappa}$

In this section we use the notation $m(i)$ for one of the conjugates corresponding to the irreducible polynomial $f_i(y)$. The rest of the conjugates corresponding to the same polynomial are $[m(i)]^p, ..., [m(i)]^{p^{\ell-1}}$.

The Hilbert space $H_A$ in Eq.(65) can be written as the direct sum of the spaces $\mathfrak{H}_{X\kappa}$ which are defined as follows. We take one position state from each of the $\ell$-dimensional spaces $H_{Xi}$ in Eq.(64) and introduce the $s$-dimensional space:

$$\mathfrak{H}_{X0} \; = \; \text{span}\{|X; m(0)\rangle, ..., |X; m(s-1)\rangle\} \tag{75}$$

Since each of the $m(0), ..., m(s-1)$ corresponds to a different irreducible polynomial, there are no Galois conjugates among them. Acting with powers of $\mathcal{G}$ on $\mathfrak{H}_{X0}$ we get the following 'copies' of $\mathfrak{H}_{X0}$:

$$\mathfrak{H}_{X\kappa} \; = \; \text{span}\{|X; [m(0)]^{p^\kappa}\rangle, ..., |X; [m(s-1)]^{p^\kappa}\rangle\} \tag{76}$$

It is easily seen that

$$H_A = \bigoplus_{\kappa=0}^{\ell-1} \mathfrak{H}_{X\kappa} \tag{77}$$

We call $\Sigma_{X\kappa}$ the projection operator to the space $\mathfrak{H}_{X\kappa}$.

We construct briefly a quantum formalism analogous to the one presented in section 3 for each of the $s$-dimensional spaces $\mathfrak{H}_{X\kappa}$. Here the states $|X; [m(\lambda)]^{p^\kappa}\rangle$ play the role of 'position states' labeled with $\lambda \in \mathcal{Z}_s$; the dual ('momentum') states are defined through a Fourier transform $\mathfrak{F}_\kappa$ which is defined below; and the phase space is $\mathcal{Z}_s \times \mathcal{Z}_s$.

In $\mathfrak{H}_{X\kappa}$ we introduce the Fourier transform:

$$\mathfrak{F}_\kappa = s^{-1/2} \sum_{\lambda,\mu} \Omega(\lambda\mu) |X; [m(\lambda)]^{p^\kappa}\rangle\langle X; [m(\mu)]^{p^\kappa}|; \quad \lambda, \mu \in \mathcal{Z}_s$$

$$\Omega(\lambda) \equiv \Omega^\lambda = \exp\left[i\frac{2\pi\lambda}{s}\right]; \qquad \mathfrak{F}_\kappa^4 = \Sigma_{X\kappa} \tag{78}$$

Clearly the Fourier transform $\mathfrak{F}_\kappa$ is very different from the Fourier transform $F$ of Eq.(41).

We define displacement operators in $\mathfrak{H}_{X\kappa}$ as

$$\mathcal{S}_\kappa = \sum_{\lambda\in\mathcal{Z}_s} |X; [m(\lambda+1)]^{p^\kappa}\rangle\langle X; [m(\lambda)]^{p^\kappa}|$$

$$\mathcal{R}_\kappa = \mathfrak{F}_\kappa \mathcal{S}_\kappa \mathfrak{F}_\kappa^\dagger = \sum_{\lambda\in\mathcal{Z}_s} \Omega^\lambda |X; [m(\lambda)]^{p^\kappa}\rangle\langle X; [m(\lambda)]^{p^\kappa}| \tag{79}$$

In analogy with Eqs(37), we can show that the $\mathcal{S}_\kappa$, $\mathcal{R}_\kappa$ form a Heisenberg-Weyl group:

$$\begin{aligned} &\mathcal{S}_\kappa^\lambda \mathcal{R}_\kappa^\mu = \mathcal{R}_\kappa^\mu \mathcal{S}_\kappa^\lambda \Omega(-\lambda\mu); \qquad \lambda, \mu \in \mathcal{Z}_s \\ &\mathcal{S}_\kappa^s = \mathcal{R}_\kappa^s = \Sigma_{X\kappa} \end{aligned} \tag{80}$$

We act with $\mathfrak{F}_\kappa$ on the $\ell$ position states of Eq.(64) and we get the dual states:

$$|\mathfrak{P}; [m(\lambda)^{p^\kappa}\rangle = \mathfrak{F}_\kappa |X; [m(\lambda)]^{p^\kappa}\rangle = s^{-1/2} \sum_{\mu \in \mathcal{Z}_s} \Omega(\lambda\mu) |X; [m(\lambda)]^{p^\kappa}\rangle \tag{81}$$

They can be viewed as 'momentum states' within the space $\mathfrak{H}_{X\kappa}$; but they are very different from the states $|P; m\rangle = F|X; m\rangle$. In analogy to Eqs(35),(36) we get:

$$\begin{aligned} &\mathcal{S}_\kappa |X; [m(\lambda)]^{p^\kappa}\rangle = |X; [m(\lambda+1)]^{p^\kappa}\rangle \\ &\mathcal{S}_\kappa |\mathfrak{P}; [m(\lambda)]^{p^\kappa}\rangle = \Omega^{-\lambda} |\mathfrak{P}; [m(\lambda)]^{p^\kappa}\rangle \end{aligned} \tag{82}$$

and also

$$\begin{aligned} &\mathcal{R}_\kappa |X; [m(\lambda)]^{p^\kappa}\rangle = \Omega^{\lambda} |X; [m(\lambda)]^{p^\kappa}\rangle \\ &\mathcal{R}_\kappa |\mathfrak{P}; [m(\lambda)]^{p^\kappa}\rangle = |\mathfrak{P}; [m(\lambda+1)]^{p^\kappa}\rangle \end{aligned} \tag{83}$$

We also introduce the 'position' operator in $\mathfrak{H}_{X\kappa}$

$$\mathfrak{r}_\kappa = \sum_{\lambda \in \mathcal{Z}_s} \lambda |X; [m(\lambda)]^{p^\kappa}\rangle\langle X; [m(\lambda)]^{p^\kappa}| \tag{84}$$

and its dual

$$\begin{aligned} \mathfrak{g}_\kappa &= \mathfrak{F}_\kappa \mathfrak{g}_\kappa \mathfrak{F}_\kappa^\dagger = \sum_{\lambda \in \mathcal{Z}_s} \lambda |\mathfrak{P}; [m(\lambda)]^{p^\kappa}\rangle\langle \mathfrak{P}; [m(\lambda)]^{p^\kappa}| \\ &= \frac{1}{2\pi i s} \sum_{\lambda,\mu} \Delta_1(\lambda-\mu) |X; [m(\lambda)]^{p^\kappa}\rangle\langle X; [m(\mu)]^{p^\kappa}| \end{aligned} \tag{85}$$

The function $\Delta_1(\lambda)$ is defined as

$$\Delta_1(\lambda) = 2\pi i \sum_{m=0}^{s-1} m\Omega(m\lambda) \tag{86}$$

It is explained in [11] that it is the analogue of the first derivative of delta function in the present context. The operators $\mathfrak{r}_\kappa$ and $\mathfrak{g}_\kappa$ are very different from the position and momentum operators $\hat{x}$ and $\hat{p}$ in Eqs(45),(46). In analogy with Eq.(34) we show that

$$\mathcal{R}_\kappa = \Omega^{\mathfrak{r}_\kappa}; \qquad \mathcal{S}_\kappa = \Omega^{-\mathfrak{g}_\kappa} \tag{87}$$

We note that acting with $\mathcal{G}$ on both sides of the various operators that we defined above in $\mathfrak{H}_{X\kappa}$ we get the corresponding operators in $\mathfrak{H}_{X\kappa+1}$:

$$\begin{aligned} &\mathcal{G}\mathfrak{r}_\kappa\mathcal{G}^\dagger=\mathfrak{r}_{\kappa+1}; \qquad \mathcal{G}\mathfrak{g}_\kappa\mathcal{G}^\dagger=\mathfrak{g}_{\kappa+1} \\ &\mathcal{G}\mathcal{R}_\kappa\mathcal{G}^\dagger=\mathcal{R}_{\kappa+1}; \qquad \mathcal{G}\mathcal{S}_\kappa\mathcal{G}^\dagger=\mathcal{S}_{\kappa+1} \end{aligned} \tag{88}$$

Physically, the transformations $\mathcal{S}_\kappa$ can be implemented in a system with Hamiltonian $\mathfrak{g}_\kappa$. In this case the evolution operator $\exp(-it\mathfrak{g}_\kappa)$ becomes equal to a power of $\mathcal{S}_\kappa$ at times which are integral multiples of $t_0=2\pi/s$. In such a system, the above formalism provides information about the 'stroboscopic evolution'. For example a state which belongs in the subspace $\mathfrak{H}_\kappa$ will evolve at times $Nt_0$ (where $N$ is an integer) into another state in the same subspace. Also, the system will return to its original states at times which are integer multiples of $Nst_0$. Similar comments can be made for the transformations $\mathcal{R}_\kappa$ which can be implemented in a system with Hamiltonian $\mathfrak{r}_\kappa$.

The use of the spaces $\mathfrak{H}_\kappa$in real physical problems requires further work. Potential applications include quantum coding, other schemes to protect quantum devices from enviromental noise, quantum information processing, the magnetic translation group in condensed matter, quantum chaos, etc.

### 5.5. Example

As an example we consider the $GF(9)$ and choose the irreducible polynomial $\epsilon^2+\epsilon+2$. The various irreducible polynomials are in this case factorized as follows:

$$\begin{aligned} f_0(y)&=y^2+2y+2=(y-1-\epsilon)(y-2\epsilon) \\ f_1(y)&=y^2+y+2=(y-\epsilon)(y-2-2\epsilon) \\ f_2(y)&=y^2+1=(y-1-2\epsilon)(y-2-\epsilon) \\ f_3(y)&=y \\ f_4(y)&=y-1 \\ f_5(y)&=y-2 \end{aligned} \tag{89}$$

Eqs.(61),become in this case

$$\begin{aligned} f_0(y)f_1(y)f_2(y)&=\frac{y^9-y}{y^3-y} \\ f_3(y)f_4(y)f_5(y)&=y^3-y \end{aligned} \tag{90}$$

The Hilbert space $H$ splits into six Frobenius subspaces

$$H = H_A \bigoplus H_B; \qquad H_A = \bigoplus_{i=0}^{2} H_{Xi}; \qquad H_B = \bigoplus_{i=3}^{5} H_{Xi} \tag{91}$$

where

$$\begin{aligned} H_{X0} &= \mathrm{span}\{|X;1+\epsilon\rangle, |X;2\epsilon\rangle\} \\ H_{X1} &= \mathrm{span}\{|X;\epsilon\rangle, |X;2+2\epsilon\rangle\} \\ H_{X2} &= \mathrm{span}\{|X;1+2\epsilon\rangle, |X;2+\epsilon\rangle\} \\ H_{X3} &= \mathrm{span}\{|X;0\rangle\} \\ H_{X4} &= \mathrm{span}\{|X;1\rangle\} \\ H_{X5} &= \mathrm{span}\{|X;2\rangle\} \end{aligned} \tag{92}$$

The operator $\mathcal{G}$ is given by:

$$\mathcal{G} = \sum_{i=0}^{5} \mathcal{G}_i \tag{93}$$

where

$$\begin{aligned} \mathcal{G}_0 &= |X;1+\epsilon\rangle\langle X;2\epsilon| + |X;2\epsilon\rangle\langle X;1+\epsilon| \\ \mathcal{G}_1 &= |X;\epsilon\rangle\langle X;2+2\epsilon| + |X;2+2\epsilon\rangle\langle X;\epsilon| \\ \mathcal{G}_2 &= |X;1+2\epsilon\rangle\langle X;2+\epsilon| + |X;2+\epsilon\rangle\langle X;1+2\epsilon| \\ \mathcal{G}_3 &= |X;0\rangle\langle X;0| \\ \mathcal{G}_4 &= |X;1\rangle\langle X;1| \\ \mathcal{G}_5 &= |X;2\rangle\langle X;2| \end{aligned} \tag{94}$$

The spaces $\mathfrak{H}_{X0}$ and $\mathfrak{H}_{X1}$ are

$$\begin{aligned} \mathfrak{H}_{X0} &= \mathrm{span}\{|X;1+\epsilon\rangle, |X;\epsilon\rangle, |X;1+2\epsilon\rangle\} \\ \mathfrak{H}_{X1} &= \mathrm{span}\{|X;2\epsilon\rangle, |X;2+2\epsilon\rangle, |X;2+\epsilon\rangle\} \\ H_A &= \mathfrak{H}_{X0} \bigoplus \mathfrak{H}_{X1} \end{aligned} \tag{95}$$

In the space $\mathfrak{H}_{X0}$ the operators $\mathcal{S}_0$ and $\mathcal{R}_0$ are given by

$$\begin{aligned} \mathcal{S}_0 &= |X;\epsilon\rangle\langle X;1+\epsilon| + |X;1+2\epsilon\rangle\langle X;\epsilon| \\ &+ |X;1+\epsilon\rangle\langle X;1+2\epsilon| \\ \mathcal{R}_0 &= |X;1+\epsilon\rangle\langle X;1+\epsilon| + \Omega|X;\epsilon\rangle\langle X;\epsilon| \\ &+ \Omega^2|X;1+2\epsilon\rangle\langle X;1+2\epsilon| \\ \Omega &= \exp\left(i\frac{2\pi}{3}\right) \end{aligned} \tag{96}$$

In the space $\mathfrak{H}_{X1}$ the operators $\mathcal{S}_1$ and $\mathcal{R}_1$ are given by

$$\begin{aligned}\mathcal{S}_1 &= |X;2+2\epsilon\rangle\langle X;2\epsilon| + |X;2+\epsilon\rangle\langle X;2+2\epsilon| \\ &+ |X;2\epsilon\rangle\langle X;2+\epsilon| \\ \mathcal{R}_1 &= |X;2\epsilon\rangle\langle X;2\epsilon| + \Omega|X;2+2\epsilon\rangle\langle X;2+2\epsilon| \\ &+ \Omega^2|X;2+\epsilon\rangle\langle X;2+\epsilon| \end{aligned} \tag{97}$$

## 6. Frobenius formalism and Riemann surfaces

The Frobenius formalism led to $\ell$ copies of the space $\mathfrak{H}_{X0}$. This is similar concept to the $\ell$ sheets in a Riemann surface related to the map

$$z \rightarrow z^{1/\ell} \tag{98}$$

More generally, there are links between the Frobenius formalism in Galois theory and Riemann surfaces. They have been discussed in various contexts (e.g., [29]) and here we discuss these links in our own context.

Various analytic representations have been used in quantum mechanics (for a review see [30]). Here we show that an analytic representation of quantum states in the space $H_A$ can be defined in the $\ell$-sheeted covering of a sphere, with states in $\mathfrak{H}_{X\kappa}$ represented by functions on the $\kappa$-sheet. This analytic representation is similar to the one discussed in [31] in a model which was introduced from a Riemann surfaces point of view and did not involve Galois theory. The aim here is to show the conceptual link of this model to Galois theory. The model uses $SU(2)$ transformations and $SU(2)$ coherent states in the spaces $\mathfrak{H}_{X\kappa}$. We refer to [31] for technical details and here we present briefly only a few formulas which show the connection between Riemann surfaces and Galois theory in a quantum mechanical context. For simplicity we consider the Bose case of odd $s$; but the formalism can be extended to the Fermi case of even $s$ also.

We consider a sphere where a point is described in spherical coordinates with the angles $(\alpha, \beta)$, where $0 \leq \alpha \leq \pi$, $0 \leq \beta < 2\pi$. A sphere is topologically equivalent to the extended complex plane $C_E = C \cup \{\infty\}$ and the stereographic projection

$$z = -\tan\left(\frac{\alpha}{2}\right) e^{-i\beta}. \tag{99}$$

provides a one-to-one mapping between the two. The south pole is mapped to the point $z = 0$ and the north pole to $\infty$. The metric in the extended complex plane is

$$d\mu(z) = \frac{dz_R dz_I}{(1+|z|^2)^2} \tag{100}$$

where $z_R, z_I$ are the real and imaginary parts of $z$, correspondingly.

We next introduce the $\ell$-sheeted extended complex plane as follows. The north and south poles are branch points of order $\ell - 1$. The cuts $\mathfrak{C}_\kappa$ and the sheets $\mathfrak{S}_\kappa$ are given by

$$\begin{aligned} \mathfrak{C}_\kappa &= \{z = r\vartheta^\kappa;\ \ r \geq 0\}\,; \quad \vartheta = \exp\left(i\frac{2\pi}{\ell}\right) \\ \mathfrak{S}_\kappa &= \left\{z = r\exp(i\phi);\ \ r \geq 0; \qquad \frac{2\pi\kappa}{\ell} < \phi < \frac{2\pi(\kappa+1)}{\ell}\right\} \end{aligned} \tag{101}$$

The sheet number of a complex number $z$ is defined as

$$\tau(z) = \mathrm{IP}\left(\frac{\ell \arg(z)}{2\pi}\right); \qquad \tau(z) \in \mathcal{Z}_\ell \tag{102}$$

where IP stands for the integer part of the number. In order to find the metric in the $\ell$-sheeted extended complex plane, we replace $z$ with $z^\ell$ in Eq.(100)and we get

$$d\mu_\ell(z) = \frac{\ell^2|z|^{2(\ell-1)}}{(1+|z|^{2\ell})^2} dz_R dz_I \tag{103}$$

A state

$$|f\rangle = \sum_{\lambda,\kappa} f(\lambda,\kappa)|X;[m(\lambda)]^{p^\kappa}\rangle; \qquad \sum_{\lambda,\kappa}|f(\lambda,\kappa)|^2 = 1 \tag{104}$$

in $H_A$, is represented with the polynomial

$$f(z) = \sum_{\lambda=0}^{s-1} d(s,\lambda) f(\lambda,\tau(z)) z^{\ell\lambda} \tag{105}$$

where

$$d(s,\lambda) = \left[\frac{(2j)!}{(j+n)!(j-n)!}\right]^{1/2}; \qquad j = \frac{s-1}{2} \tag{106}$$

The function $f(z)$ in the sheet $\mathfrak{S}_\kappa$ depends only on the projection $\Sigma_{X\kappa}|f\rangle$ of the state $|f\rangle$ in the space $\mathfrak{H}_{X\kappa}$. A state which belongs entirely in the space $\mathfrak{H}_{X\lambda}$ is represented by a function $f(z)$ which is equal to zero in all sheets apart from the $\mathfrak{S}_\lambda$.

The function $f(z)$ is analytic in the interior of all sheets $\mathfrak{S}_\kappa$ and has discontinuities across the cuts $\mathfrak{C}_\kappa$ given by

$$\Delta_\kappa(z) = \sum_{\lambda=0}^{s-1} d(s,\lambda)[f(\lambda,\kappa) - f(\lambda,\kappa-1)]z^{\ell\lambda} \tag{107}$$

The scalar product is given by

$$\langle g|f\rangle = \frac{s}{\pi}\int_{C_E}[g(z)]^* f(z)(1+|z|^{2\ell})^{1-s}d\mu_\ell(z) \tag{108}$$

The Frobenius transformations $\mathcal{G}$ are easily implemented in this representation as follows. If $f(z)$ represents the state $|f\rangle$ then

$$\mathcal{G}^\kappa|f\rangle \ \rightarrow \ f(z\vartheta^\kappa) \tag{109}$$

The above analytic representation shows that there is an interesting relation between the Frobenius formalism in Galois theory and Riemann surfaces. More work is required in this direction, with more complicated quantum systems and more complex Riemann surfaces.

## 7. Discussion

Galois fields have been introduced in quantum mechanics with a clear physical motivation: in order to have well defined symplectic transformations; or in the context of mutually unbiased bases; or in the context of quantum coding.

The motivation in this article is more mathematical and aims to bring a concept similar to field extension in the context of Hilbert spaces. Field extension constructs large fields from smaller ones. We started with a 'small' Hilbert space $\mathcal{H}$ describing a system where the position and momentum take values in the field $\mathcal{Z}_p$. Through tensor product we constructed a 'large' Hilbert space $H$ with the Fourier transform $F$ of Eq.(43), describing a system where the position and momentum take values in the Galois field $GF(p^\ell)$. This Galois quantum system is different from another quantum system with the same Hilbert space $H$ but with Fourier transform $\mathcal{F}\otimes ...\otimes\mathcal{F}$ of Eq.(44) and positions (and momenta) in $\mathcal{Z}_p\times ...\times\mathcal{Z}_p$.

Galois quantum system 'inherit' properties from Galois fields and in this paper we discussed the Frobenius formalism. We have considered the case of prime $\ell$ with a simple two-layer structure; but the discussion can be extended to all $\ell$ with a more complex multi-layer structure. We have introduced Frobenius subspaces spanned by Galois conjugate position states and we have constructed the Frobenius transformations of Eq.(66) which leave invariant these subspaces.

We have also introduced the spaces $\mathfrak{H}_{X,0},...,\mathfrak{H}_{X,\ell-1}$ (which are copies of each other) and constructed explicitly Heisenberg-Weyl groups of transformations in them. An analytic representation has been used to show the relationship of this construction to $\ell$-sheeted Riemann surfaces. Potential applications include quantum coding, quantum infor-

mation processing, the magnetic translation group in condensed matter, quantum chaos, etc.

In Galois quantum systems we have blended the areas of Galois fields and quantum mechanics. This is interesting from a mathematical point of view; and at the same time it might have several applications.

## References


1. H. Weyl, Theory of Groups and Quantum Mechanics (Dover, New York, 1950)
2. J. Schwinger, Proc. Nat. Acad. Sci. U.S.A. 46, 570 (1960); Quantum Kinematics and Dynamics (Benjamin, New York, 1970).
3. L. Auslander, R. Tolimieri Bull. Am. Math.Soc. 1, 847 (1979)
4. J.H. Hannay, M.V. Berry, Physica 1D, 267 (1980)
5. R. Balian and C. Itzykson, C.R. Acad. Sci. 303, 773 (1986)
6. D.B. Fairlie, P. Fletcher, C.K. Zachos, J. Math. Phys. 31, 1088 (1990)
7. A. Vourdas, Phys. Rev. A41, 1653 (1990)
   A. Vourdas, Phys. Rev. A43, 1564 (1991)
   A. Vourdas, C. Bendjaballah, Phys.Rev. A47, 3523 (1993)
8. A. Vourdas, J.Phys.A29, 4275 (1996)
   A. Vourdas, J.Phys.A38, 8453 (2005)
9. M. Neuhauser, J. Lie Theory 12, 15 (2002)
10. J.P. Paz, Phys. Rev. A65, 062311 (2002)
11. A. Vourdas, Rep. Prog. Phys. 67, 267 (2004)
12. J.W.P. Hirschfeld, 'Projective geometries over finite fields' (Oxford University Press, Oxford, 1979)
    L.M. Batten, 'Combinatorics of finite geometries' (cambridge University Press, Cambridge, 1997)
13. I.D. Ivanovic, J. Phys. A14, 3241 (1981)
14. W. Wootters, Ann. Phys. (NY), 176, 1 (1987)
    W. Wootters, B.D. Fields, Ann. Phys. (NY), 191, 363 (1989)
    K. Gibbons, M.J. Hoffman, W. Wootters, Phys. Rev. A70, 062101 (2004)
15. S. Bandyopadhyay, P.O. Boykin, V.Roychowdhury, F. Vatan, Algorithmica 34, 512 (2002)
16. A.O. Pittenger, M.H. Rubin, Linear Algebra Appl. 390, 255 (2004)
    A.O. Pittenger, M.H. Rubin, J. Phys. A38, 6005 (2005)
17. A. Klappenecker, M. Rotteler, Lect. Notes Comp. Science 2948, 137 (2004)
18. P. Wocjan, T. Beth, Quantum Inf. Comput. 5, 181 (2005)
19. A. Klimov, L. Sanchez-Soto, H. de Guise, J. Phys. A38, 2747 (2005)
    A. Klimov, L. Sanchez-Soto, H. de Guise, J. Opt. B:Quantum Semiclass. Opt. 7, 283 (2005)
    J.L. Romero, G. Bjork, A.B. Klimov, L.L. Sanchez-Soto, Phys. Rev. A72, 062310 (2005)
20. M. Saniga, M. Planat, H. Rosu, J. Opt. B-Quantum Semiclass. Optics 6, L19 (2004)
    M. Saniga, M. Planat, J. Phys. A39, 435 (2006)
21. T. Durt, J. Phys. A38, 5267 (2005)
    S. Colin, J. Corbett, T. Durt, D. Gross, J. Opt. B-Quantum Semiclass. Optics 7, S778 (2005)
22. E.F. Calvao, Phys. Rev. A71, 042302 (2005)

23. I. Bengtsson, A. Ericsson, Open Syst. Inf. Dyn. 12, 107 (2005)
24. B.G. Englert, Y. Aharonov, Phys. Lett. A284, 1 (2001)
25. A. Hayashi, M. Horibe, T. Hashimoto, Phys. Rev. A71, 052331 (2005)
26. A. Asikhmin, E. Knill, IEEE Trans. Inf. Theo., 47, 3065 (2001)
27. H. Barnum, C. Crepeau, D. Gottesman, A. Smith, A. Tapp, Proceedings of the 43th Annual Symposium on Foundations of Computer Science (FOCS) (IEEE Computer Society, Los Alamitos, CA, 2002) pp 449-458
28. A. Vourdas, Phys. Rev. A65, 042321 (2002)
A. Vourdas, J. Phys. A37, 3305 (2004)
29. E. Reyssat in 'From Number Theory to Physics' Ed. M. Waldschmidt, P. Moussa, J.M. Louck, C. Itzykson, (Springer, Berlin, 1992)
30. A. Vourdas, J. Phys. A. 39, R65 (2006)
31. A. Vourdas, J. Math. Phys. 36, 4757 (1995)